From: Ron Burk
To: Microsoft ATR
Date: 1/1/02 7:58pm
Subject: Microsoft Settlement

[Text body exceeds maximum size of message body (8192 bytes). It has been converted to attachment.]

Ron Burk, Founding Member
ronburk@hightechinfo.com
HighTechInfo.com
P.O. Box 3082
Redmond, WA 98052
(425) 869-0233

This is a comment on the proposed government settlement in the Microsoft antitrust action. We believe the proposed settlement does not fall within the range of acceptability, and is not within the reaches of public interest.

This comment on the proposed antitrust settlement with Microsoft argues two things:

* That the government attorneys negotiating the settlement were unable to judge the boundaries of their own competence on technical matters, leading them to assumptions that were starkly incorrect.

* That the settlement is detrimental to national security. That is due to the fact that, contrary to the government's uninformed assumption, security software that is centralized and kept secret is much more vulnerable to attack than security that is open, public and decentralized.

Courts versus Technology

Two effects must be taken into account when assessing the technical competence with which this settlement was arrived at and accepted by the participants: the accelerating complexity of technology, and accelerating permeation of technology in society. On the one hand, the technological acceleration of the last few decades guarantees that the courts must deal with highly technical issues where government officials have no hope of holding personal competence. On the other hand, the permeation of technology into society gives its non-technical members the illusion that they understand the technology well enough to judge when they are, or are not, competent to act with common sense.

For example, when powered flight first emerged, few members of the public would have ventured any opinion about how airplanes work or are piloted. By the time passenger flight was cheap and common, however, most people formed at least some very rudimentary level of understanding about airplanes and flight. Thus, most people would apply common sense to their own limited experience of airplanes to assess that flying closer to the ground is safer than flying high, and that flying slower is safer than flying fast. Unfortunately, both of these "common-sense" reactions are exactly wrong, as all student pilots must be taught.

A more compelling example of technological surprise comes when an airplane stalls, which causes the nose of the craft to pitch downward. It is only the most obvious form of common sense that the nose of the aircraft must then be immediately pulled back up, to keep the aircraft from diving into the ground. Unfortunately, this "common-sense" response is also exactly wrong. The correct response, which must be repeatedly drilled into new pilots so that they can overcome their "common sense," is to push the nose even further down and apply more power. So powerful is this incorrect feeling of "common sense," that there have been recorded accidents caused by passengers in small aircraft seizing the controls and preventing the pilot from recovering from a life-threatening stall.

Thus, we see that well-intentioned people with a passing familiarity with some form of technology may be incapable of judging the boundaries of their own competence. Moreover, technology provides many situations

where the layperson's common-sense assessment of the correct course of action is incorrect, or even disastrous. We believe that this settlement provides an example of such a disastrous application of "common sense" being applied outside a party's areas of expertise.

In the area of computers, most everyone in government has some experience using computers. While most non-technical computer users hardly believe themselves to be experts, most have enough basic experience to feel that they at least know what the limits of their competence is. As with airplanes, this assumption is generally false, and when that incorrect assumption affects court proceedings, the results can be as disastrous as an airplane crash.

Secrecy versus Security

One of the areas where the government's team clearly was incorrect in assessing the boundaries of their own technical competence was the controversial blanket exemption for disclosing any information that "would compromise the security of antipiracy, antivirus, software licensing, digital-rights management, encryption or authentication systems." The November 9, 2001 issue of The Wall Street Journal quotes the government's Mr. James as saying that this grant was "one of those 'duh' issues", continuing "Microsoft has security protocols. Are we going to tell everyone how they work? Do you want people to get access to your credit-card information when you shop on line?"

Mr. James' common-sense response to this issue is entirely logical to the layperson - and stupendously incorrect. Mr. James is presumably not aware that the security protocol used to protect almost every Internet-based credit-card transaction is public knowledge, has been so for years, and has been studied extensively by large numbers of programmers, including those who would like nothing better than to be able to steal credit card information.

Non-technical computer users often have some personal experience with "passwords," which tends to instill a belief that secrecy and security are identical. Although it contradicts the average computer user's "common sense," security experts know that the only proven way to create security protocols that can withstand attack for any length of time is to make them public. Time and time again, the history of computer security has taught programmers that security measures that rely on secrecy (e.g., I bet no one will discover where my software stores this password) have quickly fallen to attackers. Even the security protocols historically put forward by the government itself were first exposed in detail, so that they could be studied and their weaknesses assessed before critical systems were made to rely on them.

Furthermore, Mr. James would presumably be astounded to learn that the main competitor (called Apache) to Microsoft's web server product, not only uses publicly documented protocols for security, but also provides the entire source code for the server itself. That's right, any attackers who would like to steal credit card information can freely study absolutely every bit of source code that goes into the most popular web server in use on the Internet today. Once again, the layperson's "common sense" is confounded, since the number of security vulnerabilities discovered in the completely exposed Apache web server has dwindled to a trickle, while a steady stream of security flaws continues to be exposed in Microsoft's proprietary and secretive web server. Indeed, the most virulent attacks to date on the government's own computers were implemented by exploiting security flaws in Microsoft's IIS web server (ironically, some of the computers involved in the attack belonged to Microsoft - they had neglected to install their own innumerable security patches on some of their own computers).

Even Microsoft is quite aware that secrecy is not a sound basis for security, and (eventually) learned to rely on robust, publicly examined security protocols. However, they still do use secrecy extensively in

order to prevent (via legal attacks, if necessary) competitors from creating software that is compatible with their own. Thus, when Stac sued Microsoft for violating their patents, Microsoft countersued - essentially claiming that no one could make the product in question compatible with Microsoft software unless they had reverse-engineered the necessary information, which Microsoft indeed deliberately kept secret (said secrecy offering no security, only a way to prevent competition).

Thus, although Microsoft incorporated a well-known public security protocol (called Kerberos) into Windows 2000, they "extended" it in order to deliberately render it incompatible with third-party software. Again, the goal was to prevent competition, not to benefit customers.

This is precisely the sort of thing that any remedy should eliminate, and precisely the sort of thing that the government's settlement would nanvely accept as necessary. Microsoft was no doubt happy to accept the government's ignorance about computer security and, with it, the blanket exemption that will allow them to continue to hold the power of life or death over companies that need to make their products compatible with Microsoft's monopoly products to survive.

The Interests of National Security

The same Wall Street Journal article implies that thoughts of war and terrorism influenced the settlement negotiations. Here, too, it's likely that the government was unable to assess the bounds of their grasp of the big (technical) picture.

Microsoft Passport (a so-called "single logon" service) is cited as an example where Microsoft must keep information secret. Not only is it false that Passport's security relies on keeping interoperability information secret, but Passport is ironically promising to be one of the biggest threats to national cybersecurity the United States has ever seen. Because Microsoft wants Passport to be centralized and under their control, they essentially hope to put all of the nation's passwords, credit card numbers, phone numbers, and other personal information in a single location. As it is now, a foreign hacker who wants to steal credit card numbers (or blackmail a company whose customer data he stole), must do so one company at a time. With Passport, there will be a single place where a hacker can affect all customers (if Microsoft is successful at signing everyone up, which their new Windows XP tries very hard to do). Thus, part of the system that the government hopes to prop up with their settlement is a system that could become the juiciest target for cyber-terrorists of all time.

Customers have generally failed to voluntarily select Microsoft's Passport product (despite it being free), so Microsoft has resorted again to using its monopoly powers to force a product on the marketplace. They first made using Passport a requirement for certain products, though that still failed to force a large enough number of customers to participate. Most recently, Windows XP is designed to nag, cajole, and otherwise convince nanve users that they are required to use Passport. The government's settlement, with its misguided blanket exemption for security, allows Microsoft to use their monopoly power to tie this non-competitive product to their operating system, and thereby force it on the marketplace. The result is to make the nation more vulnerable to cyber attack.

An example of why a centralized and non-open design like Passport is so vulnerable was provided on November 2, 2001, when a programmer openly demonstrated a technique for stealing any Passport user's complete information (including credit cards) simply by getting the victim to open an email message. Microsoft had to shut the Passport service down for an extended period to effect repairs. Customers relying on Passport were simply out of luck for the duration of the repairs. Imagine if everyone in the U.S. used a single service for their passwords, and

therefore most Internet work came to a halt every time Microsoft needed to fix a security bug. The Internet depends on decentralization for its robustness (it has withstood power outages, cable cuts, and even terrorist attack). Microsoft hopes to force consumers to use a service that will make much Internet use highly vulnerable to all the problems the Internet itself has survived.

Unfortunately, discovering a security bug is not necessary to shut down Passport. Because the Passport design is centralized rather than distributed, it can easily be shut down by any denial of service (DOS) attack. It is currently virtually impossible to prevent DOS attacks on the Internet (experts estimate that several DOS attacks are in progress at almost any given moment on the Internet). A DOS attack may temporarily render one, or even several web sites unusable simply by "clogging the pipes" near those sites, so that all other traffic is stopped or slowed to a devastating degree. There is virtually nothing that can be done to prevent DOS attacks in the current design of the Internet (more to the point, it is a community problem, and not something that Microsoft can affect in any way by changing their software).

The centralized design of Passport (Microsoft needs it centralized so that they can control consumers' data rather than allowing competing companies to do so) assures that it is completely vulnerable to DOS attacks. Thus, the government's settlement is helping to prop up an anti-competitive single logon system that can be shut down at any time by a disgruntled teenager (often found to be the source of such attacks) with moderately high technical skills. Various arms of the government claim to be highly concerned about the threat of cyber-terrorism, yet the government proposes to accept a settlement that will prop up a monopoly's plan to build the most enticing and vulnerable cyber-terrorism target in U.S. history.

It is our belief that Passport is one of a great many areas of Microsoft anti-competitive activity that this settlement will have no effect on.

Samba: Canary in a Coal Mine

Non-technical observers typically deem the impact of any antitrust action against Microsoft likely to be difficult to measure or prove. Technical observers, however, can point to any number of concrete situations that are entirely dictated by whether or not Microsoft can continue to abuse its monopoly power.

Samba provides a good case in point. Microsoft sells server software that provides file sharing, and security management (among other things). Microsoft has, of course, tried to make their networking software largely proprietary, so that they can control who is, or is not, allowed to create compatible software. Samba is the name of a product that tries to allow users of non-Microsoft operating systems to expose services (such as file sharing) compatibly with Microsoft networks. Thus, a company that has both Unix and Windows computers can run Samba on their Unix computers to allow Windows users to easily access Unix files.

The problem with Samba is quite simply Microsoft's refusal to document their protocols. Thus, with each new release of Windows, Microsoft changes their protocols, and the Samba team has to tediously reverse engineer all the changes (just one example of the huge amount of American productivity that is wasted nationwide on reverse-engineering interfaces that Microsoft refuses to document). Microsoft knows full well that Samba will be able to eventually make their software compatible (secrecy and security being two separate things, as described earlier), but by constantly making changes and keeping Samba one step behind, they can convince companies that Samba is an inferior choice for any company that has workers using Windows.

Any antitrust settlement that allows this situation, in which Microsoft can use its standard anti-competitive techniques to keep Samba from ever catching up to "complete" compatibility with Windows, is a failure. Some believe that Microsoft will also patent their incompatibilities and then use legal means to prevent Samba from fully interoperating with Microsoft products. All of which may be perfectly acceptable in a competitive marketplace, but not in a marketplace dominated by a single monopoly.

We believe that this is just one example of the many important areas that the government-accepted settlement will allow Microsoft to practice business as usual. An integral part of what Samba does is password management. Microsoft should be able to claim to any government overseer that their network services manage passwords, and therefore they must (as they do now) refuse to document their network protocols (despite knowing full well that said protocols will eventually be reverse-engineered, and that that results in no compromise of security).

Astoundingly, the proposed settlement lets the convicted company help choose the members of its own somewhat toothless overseeing "technical committee." That fact, combined with Microsoft's prodigious ability to delay and dissemble, and the settlement's incomprehensible restriction of terms to the oddly defined "middleware" should allow Microsoft to continue to press their anti-competitive tactics on products such as Samba.

It is our belief that Samba is another one of the great many areas of Microsoft anti-competitive activity that this settlement will have no effect on.

Summary

We believe the government likely also exceeded the bounds of their competence in the area of economics. Another subtext of the negotiations (and one Microsoft pressed relentlessly in public), was that Microsoft's success is crucial to the economy. In fact, Microsoft's monopoly has consistently wiped out small businesses and innovation of all sorts for years, decimating what was once a thriving sector of the economy. Another recent Wall Street Journal article predicted that the current lack of innovation in technology would help prevent any economic turnaround in that sector. We believe that a settlement that vigorously curtailed Microsoft's ability to exploit its monopoly (which is obviously not what this proposed settlement does) would greatly stimulate the technology sector of the economy. We have not pressed that particular issue here because our credentials are in technology, not economics.

While Microsoft's lawyers had to get their negotiating agreements approved by a qualified technical overseer (Bill Gates), the government's attorneys had no such technical authority over them. As we have shown, that clearly led government negotiators to make incorrect decisions in areas where they mistakenly believed their own common sense was sufficient.

This antitrust action was an opportunity for the government to force Microsoft to take responsibility for their past flouting of the law, and to rejuvenate an industry whose main enemy is not the current economic downturn, but the illegal actions of a single monopoly. Unfortunately, the settlement appears to be ineffectual at both penalizing past law-breaking and preventing any future law-breaking. The settlement appears to be good deal for Microsoft and a few large companies. It appears to be a very bad deal for the nation's security and economy.

Ron Burk
HighTechInfo.com, www.hightechinfo.com